DEC STD 205-1 Product Fault Management Specification: Hardware Design Requirements

DOCUMENT IDENTIFIER: A-DS-EL00205-01-0000 Rev A, 10-Jul-1992

ABSTRACT: This section defines the format and content of the Product Fault Management Specification that will be implemented for each new hardware product by its product team.

APPLICABILITY: This section applies to all hardware products that are developed or purchased by Digital and will be serviced by Digital Services.

STATUS: APPROVED 10-Jul-1992; use VTX SMC for current status.

This document is confidential and proprietary, and is the property of Digital Equipment Corporation. It is an unpublished work protected under applicable copyright laws.

© Digital Equipment Corporation. 1992. All rights reserved.

DEC STD 205-1 Product Fault Management Specification: Hardware Design Requirements

DOCUMENT IDENTIFIER: A-DS-EL00205-01-0000 Rev A, 10-Jul-1992

REVISION HISTORY:	No previous revision exists.
Document Management Category:	Digital Services Requirements (FR)
Responsible Department:	Digital Services Engineering
Responsible Person:	Mike Robey
SMC Writer:	Ellie DeVries

APPROVAL: This document has been reviewed and recommended for approval by the General Review group for its category.

Mike Robey - Digital Services Engineering

Eric Williams - Standards Process Manager

Direct requests for further information to:

Mike Robey
Use $ VTX ELF for the latest location information.

Use VTX SMC to order copies of this document from Standards and Methods Control. Send distribution questions to JOKUR::SMC or call DTN: 234-4423.

The DIGITAL logo is a trademark of Digital Equipment Corporation.

CONTENTS

1 INTRODUCTION 1
1.1 PURPOSE 1
1.2 SCOPE 1
2 FRONT MATTER 3
3 PRODUCT DESCRIPTION AND FAULT MANAGEMENT GOALS 3
3.1 PRODUCT DESCRIPTION 3
3.2 FAULT MANAGEMENT GOALS 3
4 FAULT MANAGEMENT ENVIRONMENT 3
4.1 PRODUCT FAULT MANAGEMENT IMPLEMENTATION 3
4.2 HIGHER LEVEL FAULT MANAGEMENT IMPLEMENTATION 4
4.3 REFERENCE MATERIAL 4
5 PRODUCT FAULT MANAGEMENT 4
5.1 DETECTION 4
5.2 ERROR HANDLING 5
5.3 FAULT HANDLING 5
5.4 REPORTING 5
5.5 TEST OF PRODUCT FAULT MANAGEMENT 6
6 DETECTION AT HIGHER LEVELS 6
7 ERROR HANDLING AT HIGHER LEVELS 6
7.1 ANALYSIS 6
7.2 ERROR RECOVERY PROCEDURE 7
7.3 REPORTING 7
7.4 TEST ERROR HANDLING 7
8 FAULT HANDLING AT HIGHER LEVELS 8
8.1 SINGLE-EVENT FAULT ISOLATION AND REPAIR 8
8.2 MULTIPLE-EVENT FAULT ISOLATION AND REPAIR 8
8.3 REPORTING 9
8.3.1 Fault Report 9
8.3.2 Bit-To-Bit Translation 9
8.3.3 Event Monitor And Display 9
8.3.4 Event Summary Reports 10
8.4 TEST FAULT HANDLING 10
9 BACK MATTER 10

FIGURES

1 Hardware PFMS Document Structure Overview 2

1 INTRODUCTION

This standard defines the format and content of a Product Fault Management Specification (PFMS) for a hardware product. A structural overview of a hardware PFMS document is illustrated in Figure 1. If a section in the PFMS document is not applicable to a particular product, a statement to that effect shall replace that section. A PFMS encompasses the entire process of managing faults from their detection to their logical and physical removal from the system.

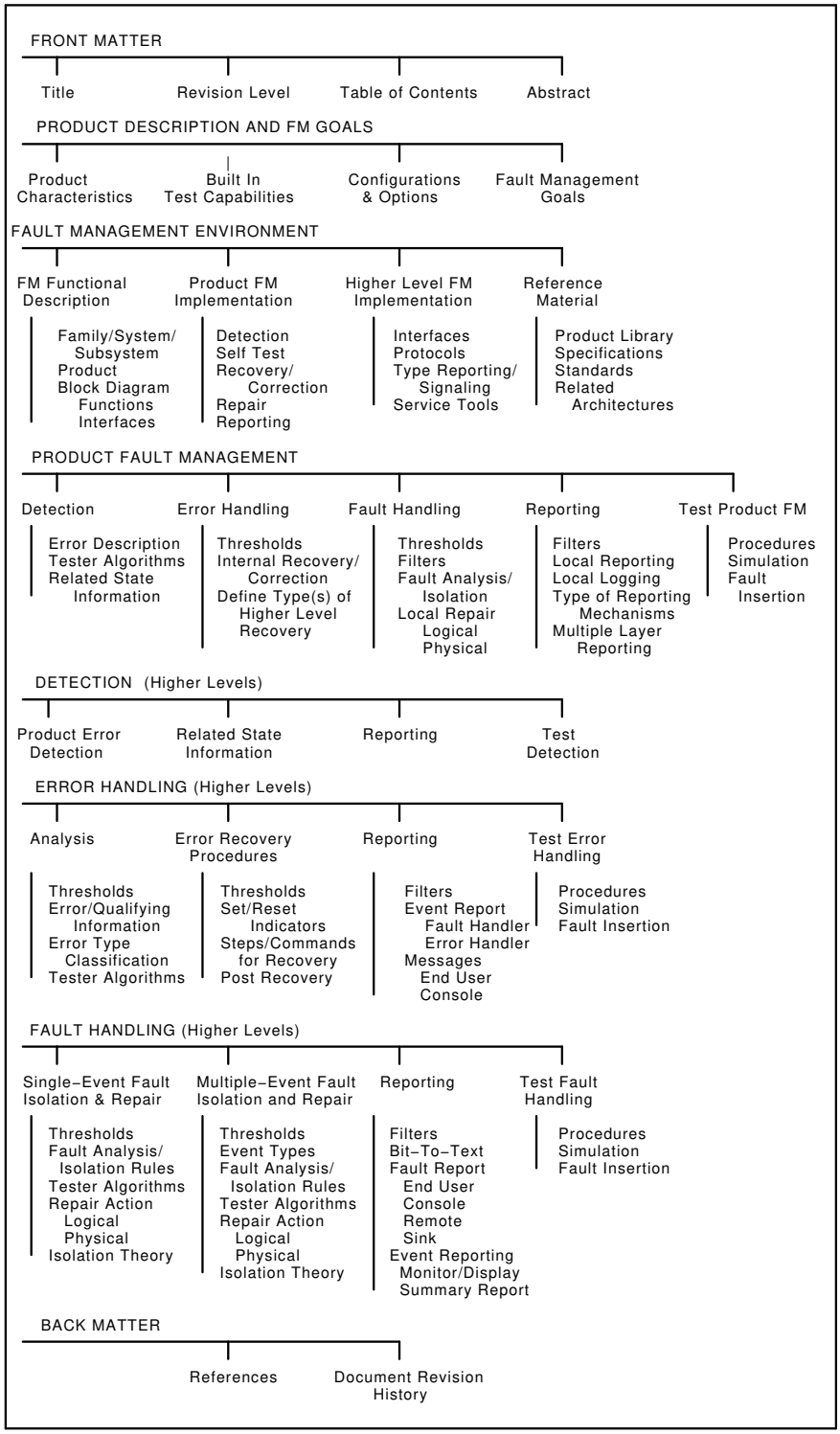
1.1 PURPOSE

This standard defines a consistent format and content for a hardware PFMS. A PFMS is used to communicate error-detection, error-handling, and fault-handling information between the product development groups, and the groups responsible for implementing operational and service support for the hardware product.

1.2 SCOPE

This standard applies to all hardware products that are developed or purchased by Digital and will be serviced by Digital Services.

Figure 1: Hardware PFMS Document Structure Overview



2 FRONT MATTER

The front matter of a PFMS document shall include a title which includes the product name and the term PFMS. The revision level of the document, a table of contents, and the abstract shall also be included as part of the front matter.

3 PRODUCT DESCRIPTION AND FAULT MANAGEMENT GOALS

A PFMS shall contain a brief description of the product and a list of product fault management goals. References should be provided that identify the specifications and documents that contain the detailed product and product-related information.

3.1 PRODUCT DESCRIPTION

The general product description shall include:

- Product physical, functional, and performance characteristics
- Built-in test capabilities
- Basic configuration and options
- Supported system entities, for example, operating systems and subsystems

3.2 FAULT MANAGEMENT GOALS

Provide the fault management goals for the product. The goals should address the following:

- Fault coverage
- Error recovery
- Fault isolation
- Service delivery tools

4 FAULT MANAGEMENT ENVIRONMENT

A PFMS shall describe functionally the fault management environments with respect to:

- The family, system, and subsystem
- The product
- Major interfaces and functional components described by use of functional block diagrams

4.1 PRODUCT FAULT MANAGEMENT IMPLEMENTATION

Describe functionally how the product will implement fault management within the fault management environment.

- Identify each type of detection mechanism and test capability used to support data intregrity, product availability, and serviceability.
- Describe functionally any error handling processes within the product.
- Describe functionally any fault handling processes within the product.

- Identify the different types of external product reporting and signaling mechanisms.

4.2 HIGHER LEVEL FAULT MANAGEMENT IMPLEMENTATION

Describe functionally how higher levels of fault management will support the product. Include in the description the following:

- The relationship between the product and each higher level of fault management.
- The types of reporting mechanisms
- The product interfaces and protocols
- How the service delivery tools will support the fault management of the product.

4.3 REFERENCE MATERIAL

Identify the reference information that is available in support of the fault management environment and where to access that information.

- A reference to the product library, if, for example, the block diagrams are part of the library.
- A list of all related family or subsystem specifications, for example, other PFMSs.
- A list of all related family or subsystem architectural documents.
- A list of standards that relate to the product's PFMS.

5 PRODUCT FAULT MANAGEMENT

Document for each detectable error the detailed information needed to provide fault management at the product level and identify the types of information required to perform higher-level product fault management. An error description should be documented in the PFMS at the time the associated detection mechanisms are proposed and should be continually updated to reflect the current state of the product. The product block diagrams should show the placement of error detectors and detection points.

The error description shall contain detection, error handling, fault handling, reporting, and test information for each detected error.

5.1 DETECTION

The error description shall include, at a minimum, the following bold faced terms to describe the detected error.

error name—A unique name that identifies the specific detected error. The name should be the same as the detected error that occurred.

error code—A code that can be used as a quick reference to the class or type of detected error. This code should be unique and consistent across similar products within the same architecture.

error definition—A description of the detected error.

- Identify the type of detection mechanism or test used to detect the error.

- Identify the actual detection point that indicated the error, for example: component, signal name, software, or firmware routine.
- Describe in a few sentences the relevant operations and states before, during, and after the detection of the error.
- Describe specific detected errors that can cause other errors, or are the result of another error.

related state information—Identify all related state information required to support fault management of the detected error. Describe how and where to obtain each item of related state information.

5.2 ERROR HANDLING

The error description shall include, at a minimum, the following bold faced terms to describe the detected error.

internal error recovery and correction—Describe any product internal error handling for the detected error:

- Identify any types of internal error recovery and correction procedures used.
- Identify any threshold values used to classify errors and note if the classification information is to be included in an event report, for example: recoverable, unrecoverable and fatal error thresholds.

external error recovery and correction—Describe briefly the types of external higher level error recovery and correction procedures that are required for the detected error. The detailed error recovery and correction procedures are specified under head 7. Error Handling at Higher Levels.

5.3 FAULT HANDLING

The error description shall include, at a minimum, the following bold faced terms to describe the detected error.

fault isolation—Provide a detailed description of all known causes of the error. This description should include the field replacement unit (FRU), for example, module, component, cables, and so forth. Provide a list of multiple FRUs in the order of the most likely to the least likely, if there are mutiple FRUs identified. The detailed higher-level fault-isolation procedures are specified under head 8. Fault Handling at Higher Levels.

local repair—Identify any physical or logical repair actions performed at the product level. Identify any filters or threshold values used in determining when to initiate a repair action at the product level.

5.4 REPORTING

The error description shall include, at a minimum, the following bold faced terms to describe the detected error.

local reporting—Identify under what conditions messages are to be sent by the product to other entities, for example, console and user terminal.

local logging—Identify under what conditions and where an error is to be logged within the product.

external reporting and signaling mechanisms—Identify the type of mechanism or program used to report or signal the detected error external to the product. Identify any mutiple reporting and signaling layers, for example, error handler to error handler, fault handler to fault handler. Document any product filters or threshold values used to suppress reporting or signaling to higher levels.

5.5 TEST OF PRODUCT FAULT MANAGEMENT

The error description shall include, at a minimum, the following bold faced term to describe the detected error.

test—Describe the test procedure required to evaluate the detection mechanism associated with the detected error. Provide the information needed to initiate the error through simulation and the information needed to interpret the results of each stage of product fault management. If the error cannot be simulated, a description shall be provided on how to cause the error through either the tester component or a fault insertion mechanism, where possible.

6 DETECTION AT HIGHER LEVELS

A PFMS shall contain the information required by a higher level to provide error detection for each class or type of error that can not be detected by the product. For example, system, subsystem, device driver, and transaction monitor. The information should include the following:

- The type of mechanism or test.
- Any related state information to be collected.
- Any algorithms to be used to initiate the detection mechanism through simulation, fault insertion, or tester component.
- Any reporting filters.

7 ERROR HANDLING AT HIGHER LEVELS

Implement error handling for each class or type of error, providing information required by a higher-level system, subsystem, device driver, or transaction monitor. If the higher-level recovery for this product is the same as an existing implementation, reference that implementation. The error-handling information should cover analysis, error recovery, reporting, and testing of the error handling.

7.1 ANALYSIS

Document the sequence of events, from the point that the error is reported to the identification of the error recovery procedure.

- Identify the reporting and signaling mechanism used to report the initial error.
- Identify any threshold values used to classify errors and note if the classification information is to be included in an event report, for example: recoverable, unrecoverable, and fatal error thresholds.

- Identify each decision point, for example, initial error and any qualifying conditions.
- Identify any tester component algorithms required to obtain additional qualifying information.
- Identify the specific type of error recovery procedure required to present correct results to the requester of the service.

7.2 ERROR RECOVERY PROCEDURE

Document the error recovery procedures for each hierarchical level.

- Identify any flags, state indicators, functions, product states that need to be set, reset, incremented, decremented, or cleared.
- Identify the steps and commands required to perform the recovery attempt, automatic or manual.
- Identify any actions needed to be performed after the recovery attempt is completed, for example, clean up, dump, log, continue, and abort.
- Provide any notes that might help the implementor of the error recovery procedure better understand the recovery procedure.

7.3 REPORTING

Document under what conditions and where information is to be sent.

- Identify any filters required to control the reporting of event reports or messages.
- Identify where the event report will be sent, for example, fault handler and higher level error handler.
- Identify under what conditions messages are to be sent to other entities, for example, console and user terminal.

Provide a definition of each unique event report (data packet). Include for each unique event report the following information:

- Event report identification should provide a definition of each unique event.
- Format and content of the event report should provide a definition of each unique event.
- Procedures that higher-level entities shall use to gain access to the data to be collected for the event report.
- The address, bit positions, and any offset of each data element that is to be collected and included in the event report.

7.4 TEST ERROR HANDLING

Document the test procedure required to validate the error-handling procedure through simulation, fault insertion or test component.

8 FAULT HANDLING AT HIGHER LEVELS

Fault handling at higher levels consists of single-event fault isolation and repair and multiple-event fault isolation and repair.

8.1 SINGLE-EVENT FAULT ISOLATION AND REPAIR

A PFMS shall contain information required by service tool developers to implement fault handling for each error class or type. The procedures include:

1. A documented sequence of events, from error detection to the identification of the required repair action. The sequence of events includes:
   a. Error identification, for example, signal name and symptoms
   b. Each decision point, for example, initial symptoms, threshold checks, qualifying conditions
   c. Identifying any tester component algorithms required to obtain additional qualifying information
   d. Identification of the component that contains the fault, for example: the FRU or likely FRUs
   e. Identification of components (chips) where possible
   f. Identification of the logical or physical repair action
2. The identification of the associated isolation theory. The isolation theory description should include:
   - A unique isolation theory identification
   - The error identification, for example, signal name or symptoms
   - The identification of the components that contain the fault
   - The repair agent and a suggested course of action
   - The comments that might help someone reading the isolation theory to better understand the nature of error or errors

8.2 MULTIPLE-EVENT FAULT ISOLATION AND REPAIR

A PFMS shall contain the information required by service tool developers to implement fault handling based on analysis of multiple events. The procedures include:

1. A documented sequence of events, from the evaluation of multiple events against threshold settings to the final identification of the fault. The isolation procedure includes the identification of:
   a. The error or event, for example, signal name and symptoms.
   b. Each decision point, for example, event type, event counts against thresholds, any qualifying conditions and indicators.
   c. Any tester component algorithms required to obtain additional qualifying information should be identified.
   d. The component that contains the fault, for example, the FRU or likely FRUs.
   e. The logical and physical repair action.

2. The identification of the associated isolation theories. The isolation theory description should include:
   - Unique isolation theory identification, for example, theory number
   - Error identification, for example, signal name and symptoms
   - Identification of the components that contain the fault
   - Repair agent and a suggested course of action
   - Explanation that might help someone reading the isolation theory better understand the nature of the errors

8.3 REPORTING

Identify any filters required to control fault or event reporting.

8.3.1 Fault Report

Identify any additional information to be added at higher levels to the event report when making up a fault report. Include for each unique fault report the following information.

- A number report identification.
- The format and content of the fault report.
- The procedures that higher level entities shall use to gain access to the additional data to be collected.
- The address, bit positions, and any offset of each data element that is to be collected.

8.3.2 Bit-To-Bit Translation

Provide the information required to translate each data element contained in each unique event or fault report. The information should include for each entry:

- The location of data element to be translated, for example, byte or register name, bit field position or size, field value, and field name
- The data type if applicable, for example, convert to radix preferred by the end user
- The exact text to report, for example, name translation to proper label and value

8.3.3 Event Monitor And Display

Provide information required by developers of service tools to implement an on-line monitor function for each event type. The information should include:

- Rules for classification of an event into categories
- Threshold setting associated with each of the categories, if applicable
- Event type and the error or event name to be displayed

8.3.4 Event Summary Reports

Provide the service tool developers with a description of each type of event that is to be included in a summary report. The description should include:

- Type of event.
- Location of the event, for example, byte or register, bit field position or size, field value.
- Error or event name to be used in the summary report.

8.4 TEST FAULT HANDLING

Describe the test procedures required to validate the fault isolation and the reporting procedures through simulation, fault insertion, or tester component.

9 BACK MATTER

The body of the document is folled by the back matter, that should consist of the following elements:

- Appendixes
- Referenced documents
- Document revision history

```
+---------------------------------------------------------------------+
|                          READER COMMENTS                            |
|                                                                     |
| Your  comments  and suggestions  will help  Standards and Methods   |
| Control improve their services and documents.                       |
+---------------------------------------------------------------------+
```

Did you request this document? _____ If so, did it arrive within a satisfactory period of time? _____ Please comment.

What are your impressions of this document? Consider format, organization, completeness, readability, and illustrations.

————————————**FOLD ON THIS LINE**———————————————————————— -

Did you find technical or clerical errors in this document? If so, please specify the page number(s) and the error(s).

Are the instructions for the update package clear? _____
Was an index available? _____ If not, is one needed? _____
Do you have other suggestions for improving this document?

The following information is optional:

Name _____ Mailstop _____

Department _____ Node _____

Send your comments to JOKUR::PROJECTS, or fold, staple, and send this page through interoffice mail to:

```
+------------------------------+
|       READERS' COMMENTS      |
| STANDARDS AND METHODS CONTROL |
|           NRO4/D4            |
+------------------------------+
```